DE LA SALLE COLLEGE

E-SAFETY POLICY

"TURN MY EYES FROM LOOKING AT WORTHLESS THINGS; AND GIVE ME LIFE IN YOUR WAYS."

PSALM 113:97

Compiled by: The College Director	Last Reviewed: June 2026
Policy Holder: Mr M. Le Moignan	Next Revision date: June 2027
Oversight Governor: Tracey Townsend	Verification date: Lent Term 2024

Contents

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.

Consequently, we need to build in the use of these technologies in order to arm our boys with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At De La Salle College, we understand the responsibility to educate our pupils on e-safety and data security issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

De La Salle College holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage and potentially damage the reputation of the college. This can make it more difficult for our college to use technology to benefit learners.

Everybody in the College has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the college (such as PCs, laptops, smart phones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto College premises (such as laptops, mobile phones, camera phones, smart phones and portable media players, etc.).

E-Safety

Roles and Responsibilities

The E-Safety policy, supported by the college's Acceptable Use Policies (AUPs) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole college community.

Outline

College Director	Mr J Turner	collegedirector@dls-jersey.co.uk
Head Teacher	Mr N Belcher	Headteacher@dls-jersey.co.uk
Assistant Head of Primary & Designated Child Safeguarding Lead for Primary	Mr M White	m.white@dls-jersey.co.uk
SIRO	Mr S Barrett	s.barrett@dls-jersey.co.uk
DPO	Mr D Washington	d.washington@dls-jersey.co.uk
E-Safety Coordinator	Mr M Le Moignan	m.lemoignan@dls-jersey.co.uk
Network Manager	Mr D Townsend	d.townsend@dls-jersey.co.uk
Designated Child Safeguarding Lead – 6th form & Secondary	Mr A Cook	a.cook @dls-jersey.co.uk
College Designated Child Safeguarding Lead	Mr D Sharrock	d.sharrock@dls-jersey.co.uk
Police Liaison Officer	PC C Jones	SAYF@jersey.pnn.police.uk
SENCO	Mrs N Jones	n.jones@dls-jersey.co.uk
E-Safety Governor	Mrs T Townsend	t.townsend@dls-jersey.co.uk

College Director

- The College Director is responsible for ensuring that the Headteacher and other relevant staff have the resources to fulfil their duties
- The College Director provides oversight of the Headteacher and the E-safety policy

Headteacher, Senior Management Team and Governors

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites safely and appropriately.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those within the college who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The SIRO, Senior Management Team (SMT) and Governors will receive regular monitoring reports from the E-Safety Co-ordinator.

- The Headteacher and another member of the SMT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this on-line facility.
- SMT and Governors are updated by the Headteacher/SIRO/E-Safety Coordinator so that they understand the issues and strategies at our college in relation to local and national guidelines and advice.

SIRO

The SIRO is a senior member of staff who is familiar with information risks and the College's response. Typically, the SIRO should be a member of the SMT and have the following responsibilities:

- Oversee and work with the E-safety Coordinator and DPO to ensure a full holistic and cohesive approach to how information risk is managed.
- To understand how the strategic business aims and objectives of the College may be impacted by information risks.
- Ensure that they are kept up to date and briefed on all information risk issues affecting the College and any business partners.
- Meet regularly with E-safety Coordinator, DPO, IT Manager, and other staff members to ensure any risk is managed effectively.
- Oversee and co-ordinate any new e-safety or technical changes to development of the College.
- Review and agree actions in respect of identified information risks.
- Ensure that the College's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the support, escalation, resolution and/or discussion of information risk issues, policy breaches and data errors.
- To ensure and oversee that all E-safety and GDPR policies and procedures and fully implemented.
- The current SIRO in this college is Mr S Barrett (September 2019).

E-Safety Coordinator

The E-Safety Coordinator's roles and responsibilities include:

- Develop an e-safe culture throughout the college as part of safeguarding, which is in line with National/Government of Jersey best practice recommendations.
- Ensure that e-safety is clearly identified and established as part of the roles and responsibility of the SMT and Governing body.
- Act as a named point of contact on all e-safety issues and liaise with other members of staff as appropriate.
- Audit and evaluate current practice to identify strengths and areas for improvement.
- Keep up to date with current research, legislation and trends in e-safety and online activities. This may include accessing appropriate training and using a range of

approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Lead an e-safety committee and hold termly meetings to discuss internal and external e-safety issues that may have impact on the college.
- Embed e-safety in staff training and CPD by ensuring that all members of staff receive up-to-date and appropriate e-safety training (at least annually and as part of induction), which sets out clear boundaries for safe and professional online conduct.
- Ensure that there is an age and ability appropriate e-safety curriculum that is embedded, progressive, flexible and relevant, which engages children's interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.
- Ensure that the setting participates in local and national events to promote positive online behaviour, e.g., Safer Internet Day, STEM Cyber Security events.
- Ensure that e-safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Ensure there are robust reporting channels for the community to access regarding e-safety concerns, including internal, local and national support.
- To ensure that age-appropriate filtering is in place, which is actively monitored. This is also a responsibility of the Network Manager.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Work with the SIRO and DPO to ensure that practice is in line with legislation.
- Produce appropriate resources that can be used to maintain e-safety integrity throughout the college and ensure that they are widely available to all members of the college, e.g., E-Safety Incident Report Form and AUPs.
- Liaise with the local authority and other local and national bodies as appropriate.
- Review and update E-Safety Policies, Acceptable Use Policies and other procedures on a regular basis (at least annually) with stakeholder input and ensuring that e-safety is integrated with other appropriate college policies and procedures.
- Monitor and report on e-safety issues to the SIRO, SMT and Governing body and other agencies as appropriate.
- Produce, distribute and analyse data from an annual whole college e-safety survey. Two surveys are used; one for Primary and one for Secondary. Information gathered from these surveys is discussed in the e-safety committee meetings and used to further the education of teachers, students, parents and carers.
- Monitor the use of BYOD by students in VI form and those with additional needs.
- Monitor the use of college-owned devices in lessons.
- Distribute, collect and securely store AUPs for BYOD or college-owned electronic devices.
- Monitor the online reputation of the college on social networking sites.

Network Manager/ICT Support Staff

The roles and responsibilities of the Network Manager and ICT Support Staff include:

- Ensure that the college's technical infrastructure is secure and is not open to misuse or malicious attack.

- Ensure that the college meets the required e-safety technical requirements and any local/national e-safety guidance that may apply.
- Ensure that users may only access the network and devices through properly enforced password protection, ensuring that passwords are regularly changed.
- Ensure that the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single individual.
- Ensure that the use of the network, internet, VLE, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher/SIRO/E-Safety Coordinator.
- Ensure that monitoring software and systems are implemented and updated as agreed in college policies.
- Respond and act upon 'helpdesk' requests made by students and staff within an appropriate timeframe (as described on the helpdesk page).
- Attend annual events that advertise and support new technologies to ensure that systems and software within the college are up to date, e.g., BETTS Show UK.

Teaching and Support Staff

The e-safety roles and responsibilities for all teaching staff, support staff and supply staff include:

- Have an up-to-date awareness of e-safety matters and of the current college e-safety policy and practices.
- Encourage pupils to develop good habits when using ICT to keep themselves safe.
- Have read, understood and signed the college Staff Acceptable Use Policy (AUP).
- Report any suspected misuse or problems to the SIRO/E-Safety Coordinator/ Headteacher for investigation/action/sanction.
- Digital communications with students (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official college systems.
- E-safety issues are embedded in all aspects of the curriculum and other college activities.
- Pastoral staff will promote the safe use of ICT with their students and will be there to support students who require advice or come forward with an e-safety concern.
- They monitor ICT activity in lessons, extra-curricular and extended college activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current college policies with regard to these devices.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- All online teaching content must be checked before delivery to ensure that websites, online searches, images and videos are age appropriate and suitable for student viewing.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted

audience or break GDPR policy. Please see the 'Data Protection' policy for further information.

- You must not reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site.
- Online gambling, illegal activities or any activity deemed inappropriate by the college is not allowed within the college or on college devices. It is at the Headteacher's discretion which internet activities are permissible for staff and how this is disseminated.

Pupils

The following e-safety roles and responsibilities apply to students within the college:

- Students are responsible for following the internet skills that are taught during computing lessons.
- Students will follow a range of curriculum areas to teach them about e-safety.
- Students have access to the college network and technologies that enable them to communicate with others beyond the communicate environment.
- Students are responsible for using the college ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to the college systems (see Appendix).
- Students are taught to critically evaluate materials, learn good researching skills and the need to avoid plagiarism and uphold copyright regulations.
- Students must observe software copyright at all times. It is illegal to copy or distribute college software, illegal software from sources or copyright materials from electronic resources (e.g., Kerboodle).
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Students should be aware of reporting issues using the 'Confide' button on their profile.
- Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying through lessons in both PSHE and ICT. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, e.g., Parent/Guardian/Teacher/Organisations such as Childline or CEOP.
- Students will be expected to know and understand college policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand college policies on the taking/use of images, use of social networking sites and on cyber-bullying.
- Students should understand the importance of adopting good e-safety practice when using digital technologies outside of the college and realise that the college's e-safety policy covers their actions outside of the college grounds, if related to the use of an externally available web-based system, provided by the college.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual properties, which may limit what they want to do but also serves to protect them.
- Online gambling, illegal activities or any activity deemed inappropriate by the college is not allowed within the college or on college devices. It is at the Headteacher's

discretion which internet activities are permissible for students and how this is disseminated.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The college will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website information, Learning Platform information and sharing local/national notifications.

Parents/Carers are responsible for:

- Accessing the college website, learning platforms, Class Charts and online parents evening system in accordance with the relevant college Acceptable Use Policies.
- Promoting the safe use of online devices both within and outside of the College.
- Ensuring that homes are fitted with adequate online security to maintain the safety of their child. Advice is available from the college SIRO, E-Safety Coordinator and Network Manager.
- It is advised that parents recheck any websites that are recommended by staff for homework activities to check their suitability. Parents are advised to supervise work that is completed online or on an electronic device.

E-Safety in the Curriculum

PSHE and E-Safety Roadmap

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum, and we continually look for new opportunities to promote e-safety.

E-safety will be taught directly within the subjects of 'Computing' and 'PSHE'. The aspects of e-safety taught in Computing can be found within the Computing departmental handbook. The aspects of e-safety taught to students in PSHE are highlighted in the roadmap in the appendix of this document. E-Safety content is taught in accordance with UK national guidance, including *Keeping Children Safe in Education 2024,* the *Education for a Connected World 2020* framework provided by the UK Council for Internet Safety and *Jersey Online Safety Policy* outlined by CYPES.

- ☐ ***APPENDIX: E-SAFETY IN PSHE ROADMAP***

E-Safety Survey

At least once every three years, a whole college e-safety survey will be completed during the week of Internet Safety Awareness Day (February). The e-safety survey will provide insight into the students understanding of e-safety and will allow the college to direct further teaching to students and their parents/guardians.

- ☐ ***APPENDIX: E-SAFETY SURVEY***

E-Safety Skills Development

Inset for NQT/RQT/New, Supply and Support Staff

- Where appropriate, new members of staff, including NQT, RQT, Support Staff and Supply Staff, will undergo mandatory training with the colleges E-Safety Coordinator, with the support of the Network Manager.
- Where appropriate, staff will read, understand and consent to the colleges Acceptable Use Policy (AUP) as a part of their introduction.
- ☐ ***APPENDIX: E-SAFETY WALKTHROUGH FOR NQT/RQT/NEW, SUPPLY AND SUPPORT STAFF***

Training

- Staff receive regular information and training on e-safety issues in the form of child protection courses and e-safety courses. These are carried out by local and national external agencies as well as online interactive training.
- Teaching staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.
- Staff have been made aware of individual responsibilities relating to the safeguarding of children with the context of e-safety and know what to do in the event of misuse of technology by any member of the college community.
- Details of ongoing staff training can be found by speaking with the SIRO or E-Safety Coordinator. A set of online, interactive courses are assigned for this purpose to college staff each academic year.

E-Safety Communication

Letters/Newsletters/Posters/Website

In order for the latest e-safety information to be communicated to members of the college, the following will take place:

- E-safety notice board in the staff room will be updated regularly and urgent announcements will be made in the weekly Staff Briefing and/or communicated by email. This will be completed by the E-safety Coordinator or the SIRO.
- E-safety notices will be placed in the Parent Briefing occasionally, which is emailed to parents on a weekly basis. This will be completed by the E-safety Coordinator or the SIRO.
- Urgent e-safety announcements will be made to students via their weekly House assemblies.
- General e-safety announcements, updates and reminders will be shown on the College TV screens as digital posters.

Website Links

In order to learn more about e-safety, staff, parents, guardians and students can refer to the following websites. The links to these websites can be found on the new De La Salle College website.

- www.thinkuknow.co.uk
- www.parentsprotect.co.uk/internet-safety.htm
- www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
- www.internetmatters.org
- www.compareitech.com
- www.nationalonlinesafety.com
- www.parentinfo.org
- www.saferinternet.org.uk
- www.childnet.com
- www.kidsmart.org.uk
- www.digzen.org
- www.giftedgeek.co.uk/keep-children-safe-online
- www.kooth.com

Safer Internet Awareness Day

Safer Internet Awareness Day (SID) is an international event taking place in February every year, which promotes a safer and more responsible use of online technology and mobile technology by children and young people across the world.

Safer Internet Day will be included as a part of the colleges Theme of the Week (TOTW) during the month of February, as close to the date of this event as possible. The SIRO, E-Safety Coordinator or an appropriate guest speaker will discuss the importance of this day/week. This information/presentation will be rolled out in the weekly House assemblies and will be organised by the E-Safety Coordinator.

Open Day, Parents Evening and Welcome Evenings

During the course of these events, the E-safety Coordinator will be present to meet with parents to discuss the e-safety provisions that we put in place at De La Salle College. The Police Liaison Officer for the college may also be present to speak with parents on an informal basis regarding any e-safety matters both within the college and at home.

E-Safety Committee

The aim of the e-safety committee is to meet on a termly basis to discuss any updates or concerns regarding e-safety both within and outside of the college. It is designed to keep all college members up to date with the latest e-safety information and minimise the harm that could occur to college members.

The e-safety committee consists of:

- SIRO – Mr S Barrett
- E-Safety Coordinator – Mr M Le Moignan
- DPO – Mr D Washington
- College Police Liaison Officer – PC A Galvin
- College E-Safety Governor – Mr G Zambon
- College Parent Governor – Mrs T Townsend
- Network Manager – Mr D Townsend
- Child Designated Safeguarting Lead for 6th form and secondary – Mr A Cook

All minutes for these meetings are recorded and published for staff members in the staff shared area. They can be found in the 'E-Safety' folder. Important matters that arise from the meeting are passed onto the College Director via the SIRO.

Communication of Policy

- This policy will be available for all staff members to view under the 'College Documents' folder in the staff shared area.
- Where appropriate, new members of staff/NQTs/RQTs/support staff/supply staff will be expected to read this policy on initiating their contract and confirm that they have read and understood its content.
- This policy will be available for all parents/guardians to read via the College website.

Review of E-Safety Policy

- There will be an ongoing opportunity for staff to discuss any concerns/issues of e-safety with the E-Safety Coordinator or SIRO.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole college development planning.
- The policy will be amended if new technologies are adopted or the Government of Jersey change the orders or guidance in any way.
- This policy will be read, amended and approved by the Headteacher and E-Safety Coordinator annually, as guided by the dates on the cover page of this document.

Acceptable Use Policies (AUPs)

The Acceptable Use Policies for the college are checked regularly to ensure that they are up to date with the recommendations from local and national agencies.

AUP: Primary College – Student

- The Acceptable Use Policy for Primary college students is worded in such a way that all students have the ability to comprehend the information that it is stipulated.
- Pupils are expected to read and discuss this agreement with their parent/guardian and follow the terms of agreement. Any concerns or explanation can be discussed with their class teacher or the Head of Primary.
- The AUP is attached to the welcome pack that all students receive when entering the Primary school of the College.
- Any new students to the Primary school of the College will have to sign the AUP before having access to the ICT hardware and online access.
- The AUP must be agreed to upon logging in to the College network. Failing to agree to the AUP will result in the user failing to get access.

☐ ***APPENDIX: AUP: PRIMARY COLLEGE – STUDENT***
☐ ***APPENDIX: AUP: PRIMARY COLLEGE – LETTER TO PARENTS***

AUP: Secondary College – Student

- The Acceptable Use Policy for Secondary college students is worded in such a way that all students have the ability to comprehend the information that it is stipulated.

- Pupils are expected to read and discuss this agreement with their parent/guardian and follow the terms of agreement. Any concerns or explanation can be discussed with their House Tutor, the E-Safety Coordinator or the SIRO.
- The AUP is attached to the welcome pack that all students receive when entering the Secondary school of the College.
- Any new students to the Secondary school of the College will have to sign the AUP before having access to the ICT hardware and online access.
- The AUP must be agreed to upon logging in to the College network. Failing to agree to the AUP will result in the user failing to get access.

- ☐ ***APPENDIX: AUP: SECONDARY COLLEGE – STUDENT***
- ☐ ***APPENDIX: AUP: SECONDARY COLLEGE – LETTER TO PARENTS***

AUP: Staff, Support Staff, Cover Staff and Governors

- All staff members, support staff, cover staff and governors (who have access to ICT) of the college must sign the AUP before having access to the college's ICT equipment and online access.
- Any concerns or clarification should be discussed with the E-Safety Coordinator or the SIRO.
- The AUP must be agreed to upon logging in to the College network. Failing to agree to the AUP will result in the user failing to get access.

- ☐ ***APPENDIX: AUP: STAFF, GOVERNORS AND VISITORS***

AUP: Visitors to the College

- ☐ All visitors entering the college site must sign in at the main reception. Visitors will be asked to sign in on the 'InVentry' system and will be provided with a lanyard and ID with a particular clearance level. The 'InVentry' details the areas of E-Safety which must be adhered to whilst in the college.
- ☐ It is essential that any visitor who requires access to the College Network (use of a USB) or Wi-Fi (access to internet) signs the Visitors E-Safety AUP which can be found at the Main Reception.

- ☐ ***APPENDIX: VISITORS TO THE COLLEGE – SECTION OF INVENTORY REFERENCING E-SAFETY***
- ☐ ***APPENDIX: AUP: VISITORS TO THE COLLEGE***

E-Safety Breaches

A breach or suspected breach of policy by a college employee, contractor or pupil may result in the temporary or permanent withdrawal of college ICT hardware, software or services from the offending individual.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting and Incident Log

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the college's SIRO. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy noncompliance must be reported to the college's SIRO and/or the DPO.

- ☐ The e-safety incident log is on TES Learning Pathways. E-Safety incidents are logged on TES Learning Pathways by either the SIRO or the E-Safety Coordinator. Serious or reoccurring e-safety incidents and complaints are investigated by the SIRO, and other necessary staff/agencies. ***APPENDIX: E-SAFETY INCIDENT REPORT FORM***

Unsuitable and Inappropriate Activities

Unsuitable and inappropriate activities are detailed in the Appendix. The activities have been categorised based on what is acceptable/not acceptable by Jersey Law, as well as the views of De La Salle College Jersey. Any activities that take place that are not found on this list, will be deemed acceptable/not acceptable at the discretion of the Headteacher.

- ☐ ***APPENDIX: E-SAFETY UNSUITABLE AND INAPPROPRIATE ACTIVITIES***

E-Safety Breach Protocol

Responding to Illegal Incidents

Once an e-safety incident report form has been filed and it is established that the incident is of an illegal nature, then the SIRO will follow the steps outlines in the Appendix: Flowchart for Managing an E-safety Incident.

Users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be identified immediately and reported to the E-safety Coordinator or the SIRO.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Coordinator or SIRO, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see Appendix).

- ☐ ***APPENDIX: FLOWCHART FOR MANAGING AN E-SAFETY INCIDENT***

Responding to Non-illegal Incidents

Once an e-safety incident report form has been filed and it is established that the incident involves a non-illegal activity, the individual will be spoken to by either the E-safety Coordinator or the SIRO, depending on the nature of the incident.

All incidents will be logged on the E-Safety incident log on TES Learning Pathways by the E-Safety Coordinator or SIRO and the parents/guardians of the individual will be contacted.

If the incident is of a repetitive or a more severe non-illegal incident, it may be that the college's Police Liaison Officer is involved with the incident.

Issues of this nature involving staff will be dealt with similarly and may involve discussions with the Network Manager and/or the Headteacher.

Complaints

Complaints and/or issues relating to e-safety should be made to the SIRO or Headteacher. All incidents should be recorded on an e-safety incident report form.

E-Safety Risk Assessment

- Activities involving online media, images from the internet and internet research should be risk-assessed using the college's 'E-Safety Risk Assessment' form.
- Staff members are responsible for completing their own 'E-Safety Risk Assessment' or they should ask for assistance from the E-Safety Coordinator in order to complete one.
- Completed risk assessments are stored within the 'E-Safety' situated in the Staff Shared area. Staff members have access to these.
- ☐ ***APPENDIX: E-SAFETY RISK ASSESSMENT FORM***

Storing/Transferring Personal, Sensitive, Confidential or Classified Information

The storage and transfer of personal, sensitive, confidential or classified information is covered in the Data Protection Policy.

Equal Opportunities

Pupils with Additional Needs

The college endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the college's e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities must be planned and well managed for these children and young people. If there is any doubt over how these conversations can be delivered clearly, please speak to the College SENCO.

Infrastructure

College Hardware

Staff Computers/Laptops

Staff computers, staff files and personal devices being used for work purposes have the right to be monitored or checked at the discretion of the Headteacher if there is an issue relating to E-safety. Staff files are checked by the Network Manager annually.

ICT Suites

Students using the ICT suites should be monitored by a staff member at all times, depending on their year group. Student workstations should be monitored by the staff member present by

visual checks or using Impero station. Students are protected by the college filtering systems (Smoothwall and Impero).

Printing/Scanning/Faxing

Staff have individual codes to access the printing and scanning services within the college. Staff should not share these codes with others and should only use their own codes.

Portable Hardware

Bring Your Own Device (BYOD)

Students in Sixth Form have the option to bring in their own electronic device that can be used for work purposes and can be connected to the college Wi-Fi network. Students have the option of using a laptop or a tablet, however, mobile phones are not accepted devices.

Students with specific educational needs can also apply to bring in and use their own electronic device with the permission of the SENCO and E-Safety Coordinator.

For further information, including the Acceptable User Policy (AUP) for the use of electronic devices (BYOD), please refer to the college's 'Electronic Devices' policy.

College Laptops/Electronic Devices

In reference to the information found above regarding BYOD, students who cannot provide their own device, but require one for their work, can be loaned a college device for the duration of their time in Sixth Form. Students with specific educational needs who are in the same situation can also be loaned a college electronic device.

For further information, including the Acceptable User Policy (AUP) for the use of electronic devices (BYOD), please refer to the college's 'Electronic Devices' policy.

Removable Storage/USBs

Staff/Support Staff

- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the College's responsibility nor the Network Manager's to install or maintain virus protection on personal systems.
- Teaching staff members are provided with an encrypted removable storage device within their welcome pack to the college. This is the only removable storage device that will function and should be used by staff if required.
- Any material that has been transferred to removable storage must be stored securely.
- Any removable media that may hold personal data (of any sort), should be disposed of securely as stated in the Data Protection policy.
- Encrypt all files containing personal, sensitive, confidential or restricted data.

- Ensure hard drives from devices no longer in service are removed and stored securely or wiped clean.

Supply Staff/Interviewees/Guest Speakers

- Supply staff, interviewees and guest speakers will not be able to use personal removable storage on the college devices.
- Individuals can plug their own electronic devices into the projectors in order to use their own removable storage or deliver material directly from the device. Material must be checked by the individual to see that it is appropriate for College use.
- Individuals can send in the material in which they wish to use/deliver in order for it to be checked and put onto the shared area. Material should be passed on to the Network Manager or ICT Support Staff for this to be done.

Students

- Students must use the college's email or remote access facilities to transfer work. They must not bring in work on removable storage devices. These will not work within the College.

Disposal of Redundant ICT Equipment

All redundant ICT equipment that may have held personal data will have the storage media removed to ensure the data is irretrievably destroyed. Or if the storage media has failed, it will be physically destroyed.

The college maintains an inventory of all its ICT equipment including a record of disposal. The college's disposal record will include:

- Date item disposed of
- Authorisation for disposal
- How it was disposed of e.g., waste, gift, sale
- Name of person and/or organisation who received the disposed item

Monitoring E-Safety

- Authorised staff may inspect any ICT equipment owned or leased by the College at any time without prior notice.
- Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its students, employees and contractors, without consent, to the extent permitted by law.
- Authorised staff may, without prior notice, access the email or voicemail account, where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
- Please note that personal communications using College ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.
- College internet access is controlled though the De La Salle College web filtering service.
- Staff and students are aware that college-based email and internet activity can be monitored and explored further if required.

- The College does not allow students access to internet logs.
- The College uses management control tools for controlling and monitoring workstations (as highlighted below).
- If staff or students discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety Coordinator/SIRO or teacher as appropriate.
- It is the responsibility of the Network Manager, to ensure that anti-virus protection, filtering services and monitoring software is installed and kept up to date on all college machines.
- If there are any issues related to viruses, anti-virus software, filtering services or monitoring software, the Network Manager should be informed immediately.
- Students using ICT equipment within a classroom should be physically monitored on a regular basis (teaching mobile around the classroom) to ensure that suitable activities are being completed on the device.
- Where necessary, staff members can request that students show the work being completed on their electronic device. They may request that students sit in a position within the classroom that allows for easier monitoring throughout the lesson.

☐ ***APPENDIX: MONITORING E-SAFETY ROLES AND RESPONSIBILITIES FLOWCHART***

Smoothwall

- Smoothwall software specialises in the web content filtering, safeguarding and internet security. Smoothwall will block websites and web searches which are considered to be harmful or potentially harmful to the user.
- Smoothwall software is installed on all fixed computing devices within the college.
- All computing devices (fixed, mobile, teacher and student) which are connected to the College network are protected by Smoothwall.

Impero

- Impero protects students with online safety technology, developed to identify the potential warning signs of at-risk behaviour, in line with Ofsted and ISI.
- All fixed machines are protected with Impero, allowing the real-time monitoring of online searches and keyword detection.
- All ICT suites in the College support Impero classroom management, allowing the teacher to have real-time monitoring and control of each device within the classroom.
- Impero is not supported on mobile devices, including those owned by staff or students who are connected to the College network.

Computer Viruses

- Never interfere with any anti-virus software installed on college ICT equipment that you use.
- If your machine is not routinely connected to the College network, you must make provision for regular virus updates through the Network Manager or ICT Support Staff.
- If you suspect there may be a virus on any college ICT equipment, stop using the equipment and contact the Network Manager or ICT Support Staff immediately. They

will advise you what actions to take and be responsible for advising others that need to know.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and agree to an Acceptable Use Policy to demonstrate that they have understood the College's E-Safety Policy.
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. Students have a generic class login in Reception, a weak private password in Year 1 and 2, and a strong private password from Year 3.
- Pupils are not allowed to deliberately access online materials or files on the College network of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of College networks, Bromcom systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Passwords will change every term. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic lock time for the College network should be no longer than 5 minutes**.**
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).
- In our College, all ICT password policies are the responsibility of the SIRO and all staff and students are expected to comply with the policies at all times**.**
- Always use your own personal passwords to access computer-based services.
- Make sure you enter your personal passwords each time you log on. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Passwords must contain a minimum of eight characters (alpha numeric) and include a capital or special character and be difficult to guess.
- User ID and passwords for staff and pupils who have left the College are disabled immediately and removed from the system by September 15th for Year 10, 11, 12 and 13 leavers and within one week for anyone else.
- **If you think your password may have been compromised or someone else has become aware of your password, report this to the Network Manager and to the SIRO.**

Servers

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly.
- Back-up tapes/discs must be securely stored in a fireproof container.
- Back-up media stored off-site must be secure.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access. Refrain from using public computers to use remote access.
- To prevent unauthorised access to the college systems, keep all access information such as IP addresses, usernames and passwords confidential and do not disclose them to anyone.
- Select passwords to ensure that they are not easily guessed. For example, do not use your house or telephone number or choose consecutive or repeated numbers. Refer to the section 'Passwords' in this policy.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect College information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-college environment.
- Individuals using remote access must ensure that their electronic devices are locked when not in use. The screen should not be in view of any other person.
- Remote access has a 'time-out' function so that it logs the member of staff out of remote access if there is inactivity for a period longer than 5 minutes.
- Microsoft Office college accounts must have a two-factor authentication in order for staff to access this data securely.

Virtual College

At certain times, it may be that students are required to complete distance learning and work online when outside of the College. It is therefore the College's responsibility to do what is reasonable in order to keep children safe online.

First and foremost, when asking students to distance learn and work online outside of College, the College and staff must adhere firstly and foremost to this Policy, to the Child Safeguarding Policy and the GDPR policy to maintain good practice.

An essential part of distance learning and the online teaching process will be ensuring children who are being asked to work online have very clear reporting routes in place, so they can raise any concerns whilst online. Information with regards to online learning will be emailed out to all parents to advise how online learning will operate, where resources can be found and finally to remind parents of e-safety good practice. The students must be reminded and aware that

they are able to contact their House Tutor, Head of House or other members of staff should an issue arise. Further, as well as reporting routes back to the College, students will also be signposted to age-appropriate practical support from the likes of:

Childline - for support

UK Safer Internet Centre - to report and remove harmful online content

CEOP - for advice on making a report about online abuse

This information and good practice advice for working online can be incorporated into a pro-forma email when the college is working through the Virtual School in order for each student to be aware of it on a daily basis. It can also be emailed to parents in the Primary school.

When distance learning or asking students to work online outside of the college, it is important that we are in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Other considerations which the college and staff must consider in relation to distance learning and use of online provision is as follows, but not exhaustive:

1. Staff to be aware of the Acceptable User Policy.
2. Staff to make students in their class or House group aware of the Acceptable User policy.
3. The importance to consider the age of student in your class, both in terms of the age requirements of the service/product you are using, together with their ability to participate in it.
4. Not all students will have access to technologies that will enable them to participate in distance learning or use online resources. Staff need to consider what solutions can be provided to enable them to continue learning, e.g., loan devices from the college or posting assignments/work home.
5. Consider activities carefully when planning – online access within the college will have internet content filtering systems in place that are unlikely to be replicated in the home environment. In Virtual School, students should not be directed to any forum or website, such as YouTube, which has not been fully researched by the teacher. The teacher must ensure that, to the best of their knowledge, the website page they are sending is age specific and would not allow students to come into contact with third parties or view unsuitable material. The teacher, where possible, should advise students and/or parents not to navigate away from the resource sent.
6. Members of staff may choose to create videos to share information, conduct a virtual assembly, lead a prayer or virtual worship opportunity, or provide tutorials to support remote teaching and learning. Videos should only be uploaded to the school's official Vimeo account by liaising with the Assistant Headteacher (Client Relations) or the Communications Manager, or uploaded onto Tapestry for Early Years, subject to the signed agreement with parents. No other video hosting sites should be used, and all content must comply with college's policies for safeguarding and e-safety. It should be understood that all videos will be accessible in the public domain, and commenting should not be made available on any video posted.

Any queries or concerns should be addressed with the College E-safety Co-ordinator or College SIRO.

Class Charts

Class Charts is an online platform which is used to inform students and parents of homework activities and allow effective communication to parents about other factors such as behaviour, detentions and support sessions.

- Staff must ensure that the homework details are input correctly with adequate detail and correct dates.
- Staff should ensure that support sessions and demerits being logged contain the correct student details and are written in a professional manner. Staff must not reveal details of other students in their messages when sending information to parents.
- Class Charts contains sensitive information and should only be used in a secure manner by members of staff who have been provided access.

Email

The use of email within De La Salle is an essential means of communication for both staff and pupils. In the context of college, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between colleges on different projects, be they staff-based or pupil-based, within college or international. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

Managing Email

- The college gives all staff their own email account to use for all college business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all email is filtered and logged and if necessary, all email histories can be traced. The college email account should be the account that is used for all college business.
- Under no circumstances should staff contact pupils, parents or conduct any college business using personal email addresses.
- The college requires a standard disclaimer to be attached to all external email correspondence.
- All emails should be written and checked carefully before sending, in the same way as a letter written on college headed paper. All emails to parents or guardians should be formal in nature and avoid the use of first names, even if the parent/guardian is well known to the staff member.
- Staff sending emails to external organisations, parents or pupils are advised to cc the Headteacher, Line Manager, Head of Department or Head of House.
- Pupils may only use college-approved accounts on the college system.

- Emails created or received as part of your college job will be subject to disclosure in response to a request for information.
- Secondary College students have their own individual college issued accounts. Primary College students in Key Stage 1 do not have a college email.
- The forwarding of chain letters is not permitted in college.
- All pupil email users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform the SIRO if they receive an offensive email.
- Secondary College students are introduced to email as part of the ICT Scheme of Work.
- However you access your college email (whether directly, through webmail when away from the office or on non-college hardware), all the college email policies apply.

Sending emails

- If sending emails containing personal, confidential, restricted or financially sensitive data to external third parties or agencies, refer to the section “Emailing Personal, Sensitive, Confidential or Restricted Information”.
- Use your own college email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- An outgoing email greater than twenty megabytes (including any attachments) is likely to be stopped automatically.
- College email is not to be used for personal advertising.

Receiving emails

- Check your email regularly.
- Never open attachments from an untrusted source. Consult the Network Manager first.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- Regularly clean through your emails and delete emails in the ‘Trash’ folder.

Emailing Personal, Sensitive, Confidential or Restricted Information

- Assess whether the information can be transmitted by other secure means before using email. Emailing restricted data is not recommended and should be avoided where possible.
- The use of Hotmail, Gmail or any other Internet based webmail service for sending email containing sensitive information is not permitted.
- Where your conclusion is that email must be used to transmit restricted data:
    - Obtain express consent from the Headteacher to provide the information by email
    - Exercise caution when sending the email and always follow these checks before releasing the email:

        - Verify the details, including accurate e-mail address, of any intended recipient of the information
        - Verify (by phoning) the details of a requestor before responding to email requests for information
    - Do not copy or forward the email to any more recipients than is absolutely necessary
    - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
    - Send the information as an encrypted document **attached** to an email
    - Provide the encryption key or password by a **separate** contact with the recipient(s)
    - Do not identify such information in the subject line of any email
    - Request confirmation of safe receipt
- ***Please note that any college related information sent by any email is subject to the provisions of GDPR and maybe subject to Freedom of Information Requests.***
- If in doubt about any of these issues, please contact the DPO.

Staff Folders and Shared Area

- Staff personal data should not be stored within the staff folders or shared area.
- Staff folders and the shared area should not be abused by staff or students and uploading of material onto these areas should be carefully thought through.
- Staff folders and the shared area will be monitored regularly by the Network Manager.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the college and therefore no longer have authorised access to the college's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the college has left.
- Staff members who are responsible for roles involving exam board material (AQA, OCR, Edexcel, Pearson) must regularly ensure that only current members of staff have access and that access levels are appropriate.
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access.

Telephones/Mobile Phones

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and then risk assessed before use within the college is allowed. De La Salle manages the use of these devices in the following ways so that users exploit them appropriately.

Staff/Support Staff – College Devices

- You are responsible for the security of your college mobile phone. Always set the PIN code on your college mobile phone and do not leave it unattended and on display (especially in vehicles).
- Report the loss or theft of any college mobile phone equipment immediately.
- The college remains responsible for all call costs until the phone is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your college mobile phone prior to using it.
- College SIM cards must only be used in college provided mobile phones.
- All college mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- You must not send text messages to premium rate services.
- All outgoing phone calls that are not answered should be reported to the college reception to inform them that a return phone call may take place.
- The sending of inappropriate text messages between any members of the college community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the college community.
- Where the college provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used.

Staff/Support Staff – Personal Devices

- The college allows staff to bring in personal mobile phones and devices for their own use.
- The college is not responsible for the loss, damage or theft of any personal mobile device.
- Personal devices should not be left unattended and should be locked when not in use.
- Staff must not take and/or store photos or videos of student activities or data involving students on their personal devices.
- With the exception of those working with children under 5, during the school day and on class outings/trips staff members may take their mobile phone, to be used for emergency purposes and required communication with the college.
- Only designated school devices, which include staff school phones or department/Pre-Reception and reception cameras and iPads, are to be used to take any photo within school or on outings.
- All photos/videos must be downloaded onto the school shared system and deleted.

Students – Personal Devices

- The context of 'electronic devices' includes mobile phones, laptops, gaming consoles, headphones and smart watches.
- Students are allowed to bring personal devices into the college but must not use them for personal purposes during school hours**.**
- Student devices should not be visible within the college and should be turned off.
-

- It is staff responsibility to ensure that we uphold the E-Safety Policy and challenge students where necessary in order to maintain the safeguarding protocols of the college. Staff should be proactive in seeking advice from the E-Safety Coordinator (Mr Le Moignan) or the SIRO (Mr Barrett) if required.
- It is not the intention of the college to remove or ban mobile devices, but to continue to effectively educate students on their appropriate use.
- At no stage should student mobile devices be visible around the college grounds. This behaviour should be challenged by any member of staff. Staff should be proactive in reminding students about this policy particularly on entry to the college at the start of the day as well as at the end of the day when students are leaving the college grounds. Students should not be using mobile devices until they have fully left the college grounds.
- Students in **Primary** and those in **Years 7-10** should not be using their mobile devices in the college (including school trips, external PE activities & transportation). These mobile devices should be turned off and not visible from the time students enter the college grounds and until they leave the college grounds. Any external contact that needs to be made by a student must be done via the college office.
- Students in **Years 11,12 and 13** should only use their mobile devices within a classroom at the discretion of the teacher for educational purposes. The teacher should consider all other alternatives before taking this action (i.e using a computer suite, using MS Teams etc.)
- If mobile devices are used within these lessons, a full risk assessment should be completed prior to the lesson using the college risk assessment document found in College Documents.
- Staff allowing students to listen to music (for Art lessons, Music lessons or revision) should ensure that mobile devices have a selected playlist that allows the device to be away for the remainder of the session. The staff member should be proactive in ensuring that music is of an appropriate nature. It is recommended that alternatives to this are used such as using a centralised class radio or playlist selected by the staff member.
- Staff must be proactive in ensuring that students using mobile devices in a classroom are doing so safely. Students actively using devices should have these visible for staff members to see. It is good practice for staff in this instance to be walking around and monitoring the classroom at all times whilst students have devices lying flat on the desk.
- Year 12 and 13 students are allowed to use their mobile devices in their Common Rooms within the Brother Edward building. This will be closely monitored by VI Form staff members. Their mobile devices should not be visible at any other time around the college grounds.
- Should staff not be vigilant they will firstly be reminded of the E-Safety Policy. If there are continued incidents where the E-Safety Policy is not complied with then those staff members may need to meet with the SIRO or the College Director.
- Incidents involving the use of mobile phones should be dealt with according to the Mobile Phone Incidents flowchart.
- ***APPENDIX: DEALING WITH MOBILE DEVICE INCIDENTS***
- The college is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any members of the college community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the college community.
- At no stage are photos or videos allowed to be taken whilst on the college grounds without the consent by a member of SMT or the Headteacher. In particular, no photos or videos are to be taken of students. This also applies to students wearing college uniform having photos or videos taken of them outside of the college. This would require permission from the parents of the students involved.
- Users bringing personal devices into the college must ensure there is no inappropriate or illegal content on the device. (However, we are aware that it is difficult to 'police' Smart phones).

Video Conferencing and MS Teams

- Video conferencing may be used by staff members for lessons or meeting purposes. Software such as Microsoft Teams are preferred. Staff members should be aware of the potential e-safety issues surrounding these calls and can refer to Appendix: A Guide to the Safe Use of Video Conferencing and Virtual Lessons – Staff.
- Students will be allowed the use of Microsoft Teams. Students and parents must be aware of the potential e-safety implications and refer to Appendix: A Guide to the Safe Use of Virtual Lessons – Parents & Students.

☐ ***APPENDIX: A GUIDE TO THE SAFE USE OF VIDEO CONFERENCING AND VIRTUAL LESSONS – STAFF***

☐ ***APPENDIX: A GUIDE TO THE SAFE USE OF VIRTUAL LESSONS – PARENTS & STAFF***

Copyright and Plagiarism

- All staff and students must abide to the copyright and plagiarism laws and/or regulations stated by the publisher.
- Staff are independently responsible for checking the regulations of each publisher before copying information or resources.

Web 2 and Social Networking

Web 2, including social networking sites, if used responsibly both outside and within an educational context, can provide easy-to-use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The college endeavours to deny access to social networking sites to students within school.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/email address, specific hobbies/interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students are asked to report any incidents of bullying (including cyberbullying) to the college.

Virtual Private Networks (VPNs)

- Students should not bypass the college network by using Virtual Private Network technology on either college or personal devices.
- Students found to be using VPN technology may be reported to the E-Safety Coordinator or SIRO and will be subject to the disciplinary procedure as described in the 'College Actions and Sanctions' section of this policy.
- Students should not set up private hotspots on their mobile devices to allow internet access to other individuals.

Webcams and CCTV

- The college uses CCTV for security and safety.
- The only people who can approve access to CCTV are the Headteacher (JTR), the Primary School Headteacher (GCE), the SIRO (SBT), the Head of Behaviour Management (ACK), the Designated Safeguarding Lead (DSK) and Head of Pastoral (CWN). Where one of these staff request CCTV it must be approved by another member of these staff.
- Notification of CCTV use is displayed at the front of the college.
- CCTV requests should be made using the correct requisition form that can be found in the staff room. A file of such requests will be kept by the Network Manager.
- CCTV should only be accessed by a standalone PC to keep it secure. This is in the office adjacent to that of the Head of the College.
- We do not use publicly accessible webcams in the college.
- Webcam footage is only used in a reactive manner.

Artificial Intelligence (AI)

This section outlines the core expectations for safe and appropriate use of Artificial Intelligence (AI) within the college community.
This section of the policy should be read in conjunction with:

- The **DLS College Artificial Intelligence Policy** (which outlines acceptable use in teaching, learning and operations)
- The **appendices of this document**, which provide detailed guidance on safeguarding risks, data protection, curriculum delivery, and operational controls relating to AI

Where safeguarding or online safety is concerned, this policy takes precedence.

Staff, Governor and Visitor Responsibilities

✓ Use Microsoft Co-Pilot or college-approved tools only when handling:
- Student information
- Staff data
- Reports, assessments, planning or governance documents
- Any sensitive or confidential content

✓ Model safe and ethical AI use by:
- Checking accuracy and bias
- Using age-appropriate and appropriate content
- Acknowledging AI use where relevant

✓ Promote safe student use by:
- Reinforcing that AI is a support tool, not a replacement for thinking
- Encouraging critical evaluation of AI-generated content
- Supporting healthy and balanced use

✓ Protect personal data at all times by:
- Following GDPR and college data protection policies
- Ensuring no personal or identifiable data is entered into unapproved tools

✓ Uphold academic integrity by:
- Making clear boundaries between acceptable support and misuse
- Supporting students in understanding correct use

✓ Report any concerns immediately in line with safeguarding procedures

❌ Enter personal or sensitive information into non-approved AI tools
❌ Use AI to mislead, impersonate, or deceive
❌ Share AI-generated content without verifying its accuracy and appropriateness
❌ Assume AI outputs are correct or unbiased
❌ Allow AI to replace effective teaching, learning, or professional judgement
❌ Use AI tools with students below legal age limits without appropriate safeguards

Student Responsibilities

✓ Use AI only through Microsoft Co-Pilot or college-approved tools for school-related work

✓ Use AI to support learning, for example:
- Generating ideas
- Revision and summarising
- Improving spelling and understanding

✓ Think critically by:
- Checking accuracy
- Comparing with trusted sources
- Questioning bias or assumptions

✓ Protect their identity and privacy by not sharing personal information, including:
- Names, images, or videos
- Addresses or passwords
- Information about peers or staff

✓ Maintain balanced use and independence in learning

✓ Report concerns or misuse to a member of staff

❌ Use AI to complete work dishonestly or replace their own thinking
❌ Submit AI-generated work as their own without permission
❌ Create or share AI-generated images, videos, or audio of others
❌ Use AI to bully, mock, impersonate, or harm others
❌ Upload personal or school-related information into unapproved tools
❌ Assume AI content is always correct
❌ Attempt to bypass safety systems or age restrictions

Reporting Procedures and Escalation
All AI-related incidents such as misuse, harmful output, deepfakes, data exposure must be reported through standard safeguarding systems:

- For student incidents → ClassCharts → E-Safety Incident

For all other concerns (staff, parent/guardian/general)

- Email **E-Safety Coordinator (Mr Le Moignan)** and **SIRO (Mr Barrett)**

All AI Incidents will be reviewed by the SIRO, E-Safety Coordinator and the Head of Behaviour as necessary. Incidents will be handled in accordance with the E-Safety Policy breaches protocol and the Behaviour Policy protocol. Incidents may lead to:

- Safeguarding referral
- Digital restrictions
- Behaviour sanctions
- Parent meetings
- External agency involvement (if required)

Further Guidance
Detailed information on:

- Safeguarding risks (including deepfakes and manipulation)
- Data protection requirements
- Behaviour and conduct expectations
- Curriculum delivery and student education

can be found in the **appendices of this policy**.

Appendix

E-safety in PSHE Roadmap

- See 'Staff Shared Area – College Documents – E-Safety – PSHE.

PSHE – Primary School

PSHE – Years 7-11

- Staying Safe Online (My Life on Screen)
- Online Gaming
- Grooming
- Online Addiction
- Friendships and Online Relationships

- Cyberbullying
- Online Grooming
- Child Exploitation and Online Protection
- Think Before You Share
- Child Abuse
- Self-esteem and Media

- Extremism
- Terrorism
- Radicalisation
- Media and Airbrushing
- Social Media and Online Stress

- Critical Thinking and Fake News
- Online Gaming and Gambling
- Social Media Validation
- Keeping Your Data Safe
- Child Sexual Abuse

- Screen Time
- Self-Image
- Instagram and Tik Tok
- Targeted Advertising & Data

- Screen Addiction and Studying
- Social Media vs Real Life
- Virtual Reality and Livestreaming
- Online Reputation and Digital Footprint
- Group Chats and Antibullying
- Pornography

PSHE – VI Form

Students in Years 12 will cover further aspects of the following E-Safety topics during the course of the academic year.

- Staying Safe Online and Social Media
- Online Addiction and Gambling
- Pornography

Students in Year 13 will cover further aspects of the following E-Safety topics during the course of the academic year.

- Extremism, Terrorism and Radicalisation
- Keeping Your Data Safe, GDPR and Plagiarism
- Online Reputation and Digital Footprints

E-Safety Survey

- See 'Staff Shared Area – College Documents – E-Safety – College Survey and Results'. A primary and secondary survey document can be found in this area. It is distributed to staff and students anonymously using Survey Monkey.

E-Safety Walkthrough for NQT/RQT/New, Supply and Support Staff

- See 'Staff Shared Area – College Documents – E-Safety – Inset and New Staff.

Open Evening and Welcome Evening Presentation

- See 'Staff Shared Area – College Documents – E-Safety – Welcome Evening and Open Evening.

AUP: Primary School AUP and Letter

DE LA SALLE COLLEGE
Wellington Road · St Saviour
Jersey JE2 7TH · Channel Islands

All pupils are expected to follow this agreement whenever they use school technology, including computers, tablets, and the internet.

The College uses a range of systems to help keep pupils safe when using technology. This includes:

- Filtering systems to block inappropriate content
- Monitoring systems, including keyword detection, which identify and flag unsafe or inappropriate activity
- Lessons and guidance to teach pupils how to stay safe online

Pupils are supported in understanding these rules and are reminded that they are designed to keep them safe while using technology.

If the rules are not followed, appropriate action will be taken in line with the College Behaviour and E-Safety Policies. This may include informing parents/carers and restricting access to ICT systems where necessary.

Pupils are expected to read and discuss this agreement with their parent or guardian.

☑ **Using Technology Safely**

- I will only use school ICT for school work
- I will only use my own username and password
- I will not tell anyone my password
- I will only open or change my own files

☑ **Being Kind and Respectful Online**

- I will use kind and polite language
- I will treat others with respect
- I will not send or share anything that could upset others

☑ **Searching and Content**

- I will not look for, save, or share anything unpleasant or inappropriate
- I will tell a teacher straight away if something makes me feel uncomfortable

☑ **Keeping Personal Information Safe**

- I will not share personal information (name, address, phone number, passwords)

- I will not arrange to meet anyone I talk to online

☑ **Images and Privacy**

- I will only take photos or videos when a teacher says it is okay
- I will not share photos or videos of others without permission

☑ **Artificial Intelligence (AI)**

- I will only use school-approved AI tools when a teacher says I can
- I will use AI to help me learn, not do all my work
- I will check that AI answers are correct
- I will not use AI to be unkind, trick others, or pretend to be someone else
- I will not enter personal or school information into AI tools

☑ **Cyber Safety**

- I will not try to get around school safety systems or filters
- I will follow rules that keep the school network safe

☑ **Mobile Devices**

- I will not use my mobile device unless a teacher gives permission
- I will not use my mobile device on school trips, external school events or the transportation between these events.
- I will keep it switched off and out of sight
- I will not take photos, videos, or use social media
- I understand my device may be taken if I do not follow the rules

☑ **Monitoring and Safety**

- I understand the school checks how I use ICT to keep me safe
- This includes keyword detection systems that flag unsafe words, searches, or behaviour
- I understand my parents/carers may be contacted if there are concerns

⚠️ **Understanding the Rules**

- These rules help keep me safe
- I know there will be consequences if I do not follow them

☑ **Agreement**

- I will follow these rules
- If I am unsure, I will ask a teacher
- Students should read and discuss this agreement with their parent/guardian.
- Any concerns should be raised with the Senior Investigating Risk Officer (SIRO)

AUP: Secondary School AUP and Letter

Dear Parent/Guardian

As part of our commitment to high-quality teaching and learning, students will have access to the internet and digital technologies. These tools are used to support learning, communication, and the development of essential digital skills.

The internet provides valuable educational resources; however, there are risks associated with its use. The College has robust systems in place to minimise these risks, including:

- Filtering systems to block inappropriate content
- Monitoring systems that identify potentially unsafe or inappropriate activity
- A structured online safety curriculum delivered through lessons, assemblies, and pastoral programmes

Students are expected to use technology safely, responsibly, and in line with College expectations.

Failure to follow this policy may result in sanctions, parental contact, or restrictions on access to College systems.

Pupils are expected to read and discuss this agreement with their parent or guardian.

☑ **Using School Systems**

- Only use ICT systems, including the internet and email, for school-related purposes
- Only log in using my own username and password
- Not share my login details with anyone
- Not download or install software without permission
- Not use unauthorised USB devices or external storage

☑ **Online Behaviour**

- Communicate respectfully and responsibly at all times
- Take responsibility for what I access, say, and share online
- Not access, download, or share content that is illegal, harmful, or inappropriate
- Report any upsetting or inappropriate content to a member of staff immediately

☑ **Staying Safe**

- Not share personal information (e.g. name, address, phone number, passwords, images)
- Not arrange to meet anyone I meet online
- Only use the College internet connection (no VPNs or personal mobile networks)

☑ **Images and Privacy**

- Only take or use images and videos for school purposes when given permission
- Not share images or videos of others without permission
- Respect the privacy and work of others at all times

☑ **Artificial Intelligence (AI)**

- Only use College-approved AI tools (e.g. Microsoft Copilot) for school work
- Use AI to support learning (e.g. ideas, revision, explanations), not replace my own thinking
- Always check AI-generated content for accuracy and bias
- Not submit AI-generated work as my own unless a teacher has allowed it

- Not use AI to create harmful content, impersonate others, or spread misinformation
- Not enter any personal or school-related information into unapproved AI tools
- Be able to explain how I have used AI if asked

☑ **Academic Integrity**

- Complete my own work honestly
- Not copy other students' work or use AI or online tools unfairly
- Follow teacher guidance on acceptable use of technology

☑ **Cyber Security**

- Not attempt to bypass College filtering or security systems
- Follow instructions that help keep the network safe
- Understand that my activity may be monitored for safety

☑ **Mobile Devices**

- Not use mobile devices on College grounds unless given permission by a member of staff
- I will not use my mobile device on school trips, external school events or the transportation between these events.
- Keep devices switched off and out of sight during the College day
- Not use personal devices for photos, videos, or social media in College
- Understand that devices may be confiscated if misused

☑ **Behaviour and Respect**

- Not use technology to bully, threaten, or harm others
- Not create or share harmful or offensive content (including edited or manipulated images/videos)
- Ensure my behaviour online does not harm others or damage the reputation of the College

⚠ **Monitoring and Consequences**

- I understand that my use of ICT systems is monitored and logged to keep me safe. This includes automated systems, such as keyword detection, that identify and flag unsafe or inappropriate activity, including concerning language or searches.
- I understand that breaking these rules may result in:
    - Sanctions
    - Loss of access to ICT systems
    - Parent/guardian being informed
    - Further action in line with the Behaviour Policy

☑ **Agreement**

- I will follow these rules
- If I am unsure, I will ask a teacher
- Students should read and discuss this agreement with their parent/guardian.
- Any concerns should be raised with the Senior Investigating Risk Officer (SIRO)

AUP: Staff, Support Staff, Cover Staff and Governors

ICT systems (including data), email, the internet, mobile technologies, and cloud-based platforms form an essential part of daily working practice within the College. This policy ensures that all staff understand their professional responsibilities when using ICT, both within the College and in any professional context.

All staff and governors are required to read, sign and adhere to this policy at all times. Any queries should be directed to the Senior Information Risk Officer (SIRO).

1. Acceptable Use of ICT

I agree that I will:

- Use College ICT systems for professional purposes only, or as deemed reasonable by the Headteacher/Principal.
- Ensure all electronic communication with pupils, parents and colleagues is appropriate and professional.
- Only use College-approved communication systems for school business.
- Not share personal contact details with pupils (e.g. phone number, personal email, social media).
- Not communicate with pupils via social media or messaging platforms unless explicitly authorised.

2. Data Protection & Security

I agree that I will:

- Comply fully with the College's Data Protection Policy and UK GDPR.
- Ensure personal data is stored, accessed, and shared securely at all times.
- Only take personal or sensitive data off-site when authorised by the DPO.
- Ensure any off-site data is encrypted and securely stored.
- Never share passwords or login credentials.
- Report any data breach or suspected breach immediately.

3. Systems, Software and Monitoring

I agree that I will:

- Not install hardware, software, or applications without approval.
- Not access or distribute inappropriate, illegal, or offensive material.
- Understand that use of College ICT systems may be monitored and logged.

4. Images and Media

I agree that I will:

- Only take and use images for professional purposes.
- Ensure appropriate consent is obtained.
- Not share images outside the College network without DPO approval.

5. Professional Conduct & Online Behaviour

I agree that I will:

- Maintain high professional standards online at all times.
- Ensure my conduct does not bring the College into disrepute.
- Not create or share content that could harm or offend others.
- Respect copyright and intellectual property rights.

6. Safeguarding & Online Safety

I agree that I will:

- Support the College's approach to online safety.
- Model safe and responsible use of technology.
- Report safeguarding or online safety concerns immediately.
- Support pupils in developing safe digital behaviours.

7. Artificial Intelligence (AI) Use

I understand that AI must be used safely, ethically, and in line with College policy.

I agree that I will:

- Only use Microsoft Copilot or College-approved AI tools when handling:
    - Student information
    - Staff data
    - Reports, assessments, or official documents
    - Any sensitive or confidential content
- Not enter personal or sensitive data into non-approved AI tools.
- Recognise that AI-generated content may be inaccurate or biased and will verify outputs before use.
- Accept that all AI-assisted work remains my professional responsibility.
- Not use AI to mislead, impersonate, or generate harmful or inappropriate content (including deepfakes).
- Model ethical and responsible AI use and acknowledge its use where appropriate.
- Ensure AI supports, but does not replace, professional judgement or teaching.
- Support pupils to use AI safely, critically, and appropriately.
- Report any AI-related concerns or misuse immediately.

8. Cyber Security

I agree that I will:

- Remain vigilant to phishing and cyber threats.

- Use strong passwords and authentication measures.
- Not share login details or allow unauthorised access.
- Lock devices when unattended.
- Not bypass security systems.
- Complete required cyber security training.

9. Remote Working

I agree that I will:

- Use secure, approved methods to access College systems remotely.
- Ensure screens and devices are not visible to unauthorised individuals.
- Work in a secure and private environment when handling sensitive data.
- Not store sensitive data on unsecured personal devices.

10. Use of Personal Devices (BYOD)

If using personal devices, I agree that I will:

- Ensure devices are secure and password-protected.
- Only access systems via approved platforms.
- Not store personal or sensitive data unless authorised.
- Ensure data is deleted or secured appropriately after use.

11. Monitoring and Compliance

I understand that:

- My use of ICT systems may be monitored and logged.
- Breaches of this policy may result in disciplinary action.

12. Consent

I give permission for the College to use images of me in publications in line with policy.

AUP: Visitors to the College – E-Safety Inventory and AUP

The college 'InVentry' highlights the following general E-Safety information. However, if a visitor is using the college network, then they should also sign the Visitor AUP.

Use of technology

- The college uses CCTV for security and safety.
- The college is not responsible for the loss, damage or theft of any personal electronic devices.
- Please do not use mobile phones in student accessible spaces within the college.
- Photos or videos are not to be taken which involve student activities or student data. The use of cameras and video recording in the college must be authorised by the Headmaster.
- Use of the internet on school premises should be for school use only, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business.
- No personal removable storage devices (USBs) are to be used on the college network. Any files which need transferring to the college network should be done through an encrypted USB provided by the college, sent online or transferred by the Network Manager.
- All e-safety breaches must be reported immediately to the SIRO or Headmaster.
- For more information on the use of technology within the college please refer to the E-Safety Policy.

AUP: Visitors

All visitors, contractors, governors, and external users of De La Salle College Jersey are required to read and sign this Acceptable Use Policy (AUP).

This policy outlines expectations when using College systems, networks, devices, cloud platforms, and online services, both on-site and in any professional context related to the College.

Any queries should be directed to the Senior Information Risk Officer (SIRO) or the Head of the College.

☑ Acceptable Use

I agree that I will:

- Use College ICT systems and internet access only for authorised and professional purposes
- Ensure all communication with pupils and staff is appropriate and in line with my role
- Not share personal contact details with pupils (e.g. personal phone number, email, social media)
- Not use social networking or messaging platforms to communicate with pupils

☑ Data Protection & Security

- Comply fully with the College's Data Protection Policy and UK GDPR
- Ensure personal data is kept secure and used appropriately at all times
- Only access, use, or share data where authorised
- Not share passwords or login details
- Only remove or transfer data off-site where authorised by the DPO
- Ensure any off-site data is encrypted and securely handled

☑ Artificial Intelligence (AI)

- Only use College-approved AI tools (e.g. Microsoft Copilot) when handling any school-related information
- Not enter personal, sensitive, or confidential data into unapproved AI tools
- Ensure AI-generated content is checked for accuracy, bias, and appropriateness
- Not use AI to mislead, impersonate, or create harmful or inappropriate content

☑ Systems, Devices and Network Use

- Not install hardware, software, or applications without permission
- Not use unauthorised external storage devices (e.g. USBs) on the College network
- Only transfer files using approved and secure methods
- Not attempt to bypass security, filtering, or monitoring systems

☑ Images and Media

- Only take, store, or use images of pupils or staff for approved professional purposes
- Ensure appropriate consent has been obtained
- Not share images outside the College network without DPO approval

☑ Professional Conduct

- Not access, download, or share material that is illegal, offensive, or inappropriate
- Ensure my behaviour does not bring the College into disrepute
- Respect copyright and intellectual property rights
- Support the College's approach to online safety and safeguarding

☑ Monitoring and Safety

- Understand that all use of College ICT systems may be monitored and logged
- Understand that this includes systems such as keyword detection, which identify and flag unsafe or inappropriate activity

☑ Safeguarding

- Immediately report any safeguarding, e-safety, or data protection concerns to the SIRO or Headteacher
- Follow all College safeguarding procedures

☑ On-Site Expectations

- Not use personal electronic devices in student-accessible areas unless authorised
- Understand that misuse of devices may result in action being taken
- Be aware that CCTV is in operation for safety and security
- Understand that the College is not responsible for loss, theft, or damage to personal devices

⚠ Compliance

- Understand that failure to follow this policy may result in:
    - Removal of access to College systems
    - Termination of visit or contract
    - Further action where appropriate

☑ Agreement

I confirm that I have read and agree to follow this Acceptable Use Policy.

Name: _____

Organisation: _____

Signature: _____

Date: _____

E-Safety Incident Report Form

E-Safety Incident Report Form

De La Salle College Jersey

Any e-safety incidents should be recorded on the form below. It is only the responsibility of the teacher to report the facts of the incident and not to investigate the matter themselves. All e-safety reports should be passed on to the SIRO (SBT) immediately. In the event of the SIRO not being available, the form can be passed on to a member of SMT or the Headmaster (JTR).
Any lost/stolen electronic devices or security breaches (including username/password details, remote access details, PINs and electronic door cards) must be reported to the DPO (DWN) and SIRO immediately.

Name of Teacher Reporting Incident: _____

Date of Incident: _____

Location of Incident: _____

Name of Student(s)/Staff Involved in Incident:

_____

_____

Basic Details of Incident (recorded by Teacher):

_____

_____

Date Incident Logged by Teacher: _____

Date Incident Passed onto SIRO (SBT): _____

Confirmed Signature by SIRO (SBT): _____

This section of the form is to be completed by the SIRO (SBT). The e-safety reports must be filed by the SIRO and stored securely. All e-safety incidents will be monitored by the Headmaster (JTR) and reviewed annually by the e-safety Governor (GZN). Incidents involving cyber-bullying should be passed on to anti-bullying officer (ACK).

Incident Type Number(s): _____

Detailed Description of Incident:

_____

_____

_____

_____

_____

Immediate Corrective Action:

_____

_____

_____

_____

Incident Types

1 – Circumventing the network security

2 – Installing unapproved software

3 – Using other people's profile/email/passwords

4 – Breaching copyright

5 – Uploading College material onto social network

6 – Bullying/cyberbullying or harassment

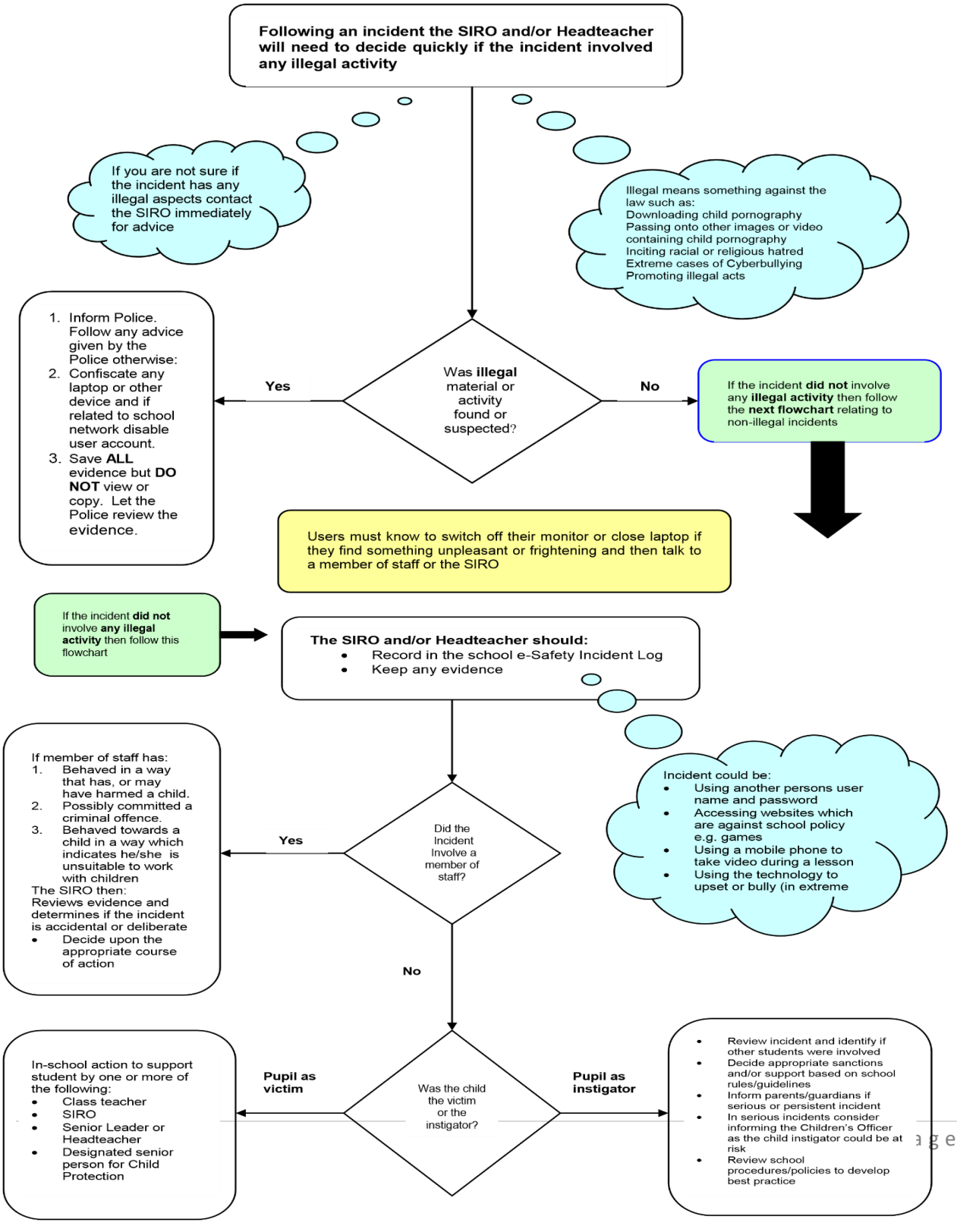
7 – Racist/sexist/homophobic comments

8 – Violence or terror related material

9 – Alcohol/drugs/smoking/vaping material

10 – Online gambling material

Flowchart for Managing an E-safety Incident



E-Safety Risk Assessment Template

- See 'Staff Shared Area – College Documents – E-Safety – Risk Assessment.

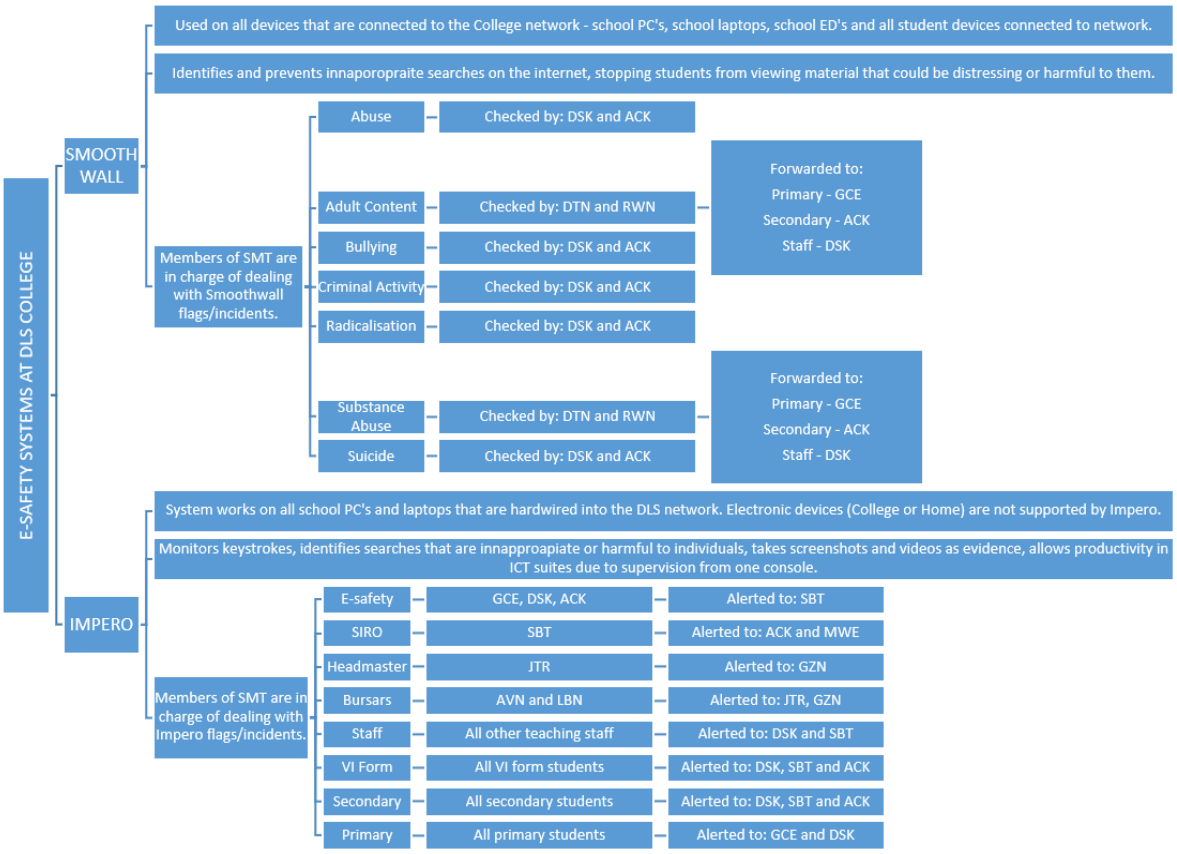
E-Safety Unsuitable and Inappropriate Activities

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Child sexual abuse images – the making, production or distribution of indecent images of children Contrary to the Protection of Children's Act 1978					**X**
Grooming, incitement, arrangement of facilitations of sexual acts against children Contrary to the Sexual Offences Act 2003					**X**
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					**X**
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) Contrary to the Public Order Act 1986					**X**
Pornography				**X**	
Promotion of any kind of discrimination				**X**	
Threatening behaviour, including promotion of physical violence or mental harm				**X**	
Any other information which may offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				**X**	
Using college systems to run a private business				**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college				**X**	
Infringing copyright				**X**	
Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)				**X**	
Creating or propagating computer viruses or other harmful files				**X**	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				**X**	
Online gaming (educational)		**X**			
Online gaming (non-educational)		**X**			
Online gambling				**X**	

Online shopping/commerce			X		
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting (e.g. YouTube, Vimeo, TES)			X		

E-Safety Monitoring Roles and Responsibilities Flowchart

- See 'Staff Shared Area – College Documents – E-Safety – Roles and Responsibilities.



Dealing with Mobile Device Incidents

- See 'Staff Shared Area – College Documents – E-Safety – Mobile Phone Incident Flowchart.

A Guide to the Safe Use of Video Conferencing and Virtual Lessons – Staff

- See 'Staff Shared Area – College Documents – E-Safety – Microsoft Teams.

A Guide to the Safe Use of Virtual Lessons – Parents and Students

- See 'Staff Shared Area – College Documents – E-Safety – Microsoft Teams.

Artificial Intelligence (AI)

Appendix A: Safeguarding Principles for AI Use

A1. Protection from Harm

AI must not expose students to:

- Emotional or psychological harm
- Reputational damage
- Bullying or harassment
- Misleading or manipulated content (e.g. deepfakes)

A2. Identity and Data Protection

- Personal data must not be entered into unapproved AI tools
- Student work, images, and identifiable information must be protected
- All use must comply with GDPR and the College Data Protection Policy

A3. Healthy Digital Behaviour

- AI should support learning, not replace independent thinking
- Over-reliance on AI must be actively discouraged

A4. Academic Integrity

- AI must not be used to complete assessed work dishonestly
- Students must develop their own skills and understanding

A5. Ethical and Transparent Use

- AI-generated content must be checked for accuracy and bias
- Use of AI should be acknowledged where appropriate

Appendix B: Key E-Safety Risks Associated with AI

B1. Deepfakes and Digital Manipulation

AI can:

- Create realistic but false images, audio, and video
- Misrepresent or impersonate individuals
- Be used to bully, harass, or humiliate

These risks are addressed through the curriculum, assemblies, and safeguarding education.

B2. Data Privacy and Security

Risks include:

- Entering personal data into AI tools
- Use of non-compliant platforms
- Storage of data outside UK/Jersey/EU legal standards

Control measure:

Only approved AI tools (e.g. Microsoft Copilot) may be used where sensitive data is involved.

B3. Accuracy, Bias and Misinformation

AI systems may:

- Produce incorrect or fabricated information
- Reinforce bias or stereotypes
- Generate inappropriate or unsafe content

All outputs must be checked against trusted sources.

B4. Wellbeing and Over-Reliance

Potential impacts include:

- Reduced independent thinking
- Lower academic performance
- Dependence on AI for decision-making

Balanced and appropriate use must be promoted.

B5. Behaviour and Conduct Risks

AI may be used to:

- Create harmful or abusive content
- Manipulate images or videos of peers or staff
- Engage in anonymous or indirect bullying

Such behaviour will be managed in line with safeguarding and behaviour policies.

Appendix C: Data Protection and GDPR Requirements

- All AI use must comply with GDPR
- Personal data must only be used within college-approved systems
- The following must not be uploaded into unapproved tools:
    - Student names, images, or identifiers
    - Assessment data or reports
    - Safeguarding, SEN, or pastoral information
- Staff must complete regular data protection training
- Any uncertainty must be referred to the SIRO or Data Protection Lead

Appendix D: Teaching, Curriculum and Awareness

AI education is embedded through:

- PSHE (KS3–KS5)
- ICT and Computing
- Safer Internet Awareness Week
- Form Time and assemblies

Students will be taught to:

- Understand how AI systems work
- Recognise deepfakes and manipulated media
- Evaluate accuracy and bias
- Use AI safely and responsibly

Appendix E: Operational and Technical Controls

E1. Filtering and Monitoring

The college will:

- Block unapproved AI platforms where feasible
- Monitor AI-related activity as part of e-safety systems
- Flag concerning searches or behaviours

E2. Devices and Network Controls

- AI features may be restricted on devices
- College devices default to approved AI tools
- Visitor access may require supervision

Appendix F: SEND and Accessibility

AI may support:

- Reading and writing
- Dictation and organisation
- Differentiation and accessibility

However, it must not:

- Replace core skill development
- Compromise assessment integrity
- Create risks to personal data protection